Nansen: спеціалізується на аналізі активності розумних грошей та відстеженні потоків капіталу. • Messari: пропонує як фундаментальні дані, так і деякі ончейн-метрики з акцентом на якість даних. • CryptoQuant: надає дані про обмінні потоки, активність майнерів та інші корисні показники. • Dune

Analytics: дозволяє користувачам створювати власні інформаційні панелі та аналізувати дані смарт-контрактів. • Etherscan, BscScan, Arbiскан та інші блокчейн-експловери: надають основну інформацію про транзакції, гаманці та смарт-контракти конкретних мереж.

Цей огляд демонструє зростаючий інтерес наукової спільноти до використання аналізу в ланцюжку для вивчення різних аспектів ринку крипто валют. Дані дослідження охоплюють широкий спектр тем, від прогнозування цін і виявлення ринкових аномалій до аналізу безпеки і фундаментальних характеристик блокчейн-мереж. Подальші дослідження в цій галузі сприятимуть більш глибокому розумінню динаміки та потенціалу крипто валютних активів.

1. Jin, M., Liu, R., & Monperrus, M. (2025). *On-Chain Analysis of Smart Contract Dependency Risks on Ethereum*. arXiv. https://arxiv.org/abs/2503.19548

2. Dalia Elbanna, Ema Izati Zull Kepili1 , Nik Hadiyan Nik Azman. *Beyond Conventional Methods: Advancing Ethereum Price Prediction through Integrated Technical, On-Chain, and Machine Learning Approaches*. INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE & MANAGEMENT SCIENCES Vol. 1 5 , No. 2, 2025, E-ISSN: 2225-8329 © 2025. https://hrmars.com/papers_submitted/24968/beyond-conventional-methods-advancing_ethereum-price-prediction-through-integrated-technical-on-chain-and_machine-learning-approaches.pdf

Розробка алгоритму перевірки інформаційної складової сайтів на фейкшопінг та фішинг

УДК 004.056.53

Софія Гіленко
Національний університет «Одеська політехніка»,
9480588@stud.op.edu.ua

Фейкові інтернет-магазини та фішингові вебсайти є одними з найпоширеніших форм онлайн-шахрайства[1], які завдають щорічно мільярдних збитків споживачам і бізнесу. Візуальна подібність таких ресурсів до легітимних магазинів, їх активна реклама в соцмережах, високоякісний дизайн і фейкові відгуки суттєво ускладнюють відрізнення шахрайських сторінок від справжніх. З іншого боку, фішинг як окремий напрям використовує соціальну інженерію, URL-омографи, маніпуляції з доменами та глибокі підробки для виманювання конфіденційних даних. У сучасних умовах, коли багато таких ресурсів працюють лише кілька днів, традиційні методи, що спираються на чорні списки чи ручну перевірку, стають неефективними[2].

Метою цієї роботи є розробка ефективного, автоматизованого алгоритму для виявлення фейкових онлайн-магазинів та фішингових ресурсів на основі комплексного аналізу вебконтенту, метаінформації та структури URL. Для цього використано мову програмування Python та набір бібліотек, зокрема: requests для отримання HTML, BeautifulSoup для парсингу структури сторінки, Scikit-learn для машинного навчання, tldextract для аналізу доменів та інші засоби роботи з вебданими.

Сформовано набір ознак, які відображають найбільш характерні властивості шахрайських сайтів. Сюди входять: відсутність HTTPS-захисту, довжина та структура доменного імені, присутність підозрілих слів у URL ("sale", "discount", "secure"), використання IP-адреси замість домену, відсутність контактної інформації на сторінці, кількість форм для введення особистих даних, повторювані шаблони HTML-структури тощо. Також враховувались часові характеристики, такі як вік домену та термін реєстрації.

Для навчання моделі використано збалансовану вибірку реальних вебсайтів, що включала як фейкові магазини й фішингові сторінки, так і легітимні ресурси популярних брендів. Було протестовано декілька моделей класифікації: Decision Tree, Random Forest, Logistic Regression, із подальшим вибором Random Forest через його стабільність, високу точність та збалансовані значення метрик, зокрема точності, повноти та F-міри[3]. Векторизацію виконано через словникове кодування категоріальних ознак та нормалізацію числових.

Результати експериментів показали точність класифікації понад 80 % при збереженні високих значень Precision і Recall. Також було проведено аналіз важливості ознак, який дозволив встановити, що найбільший внесок у детекцію дають показники URL, наявність форм авторизації, вік домену та ознаки копіпейст-дизайну. Це підтверджує практичну значущість використаних фіч.

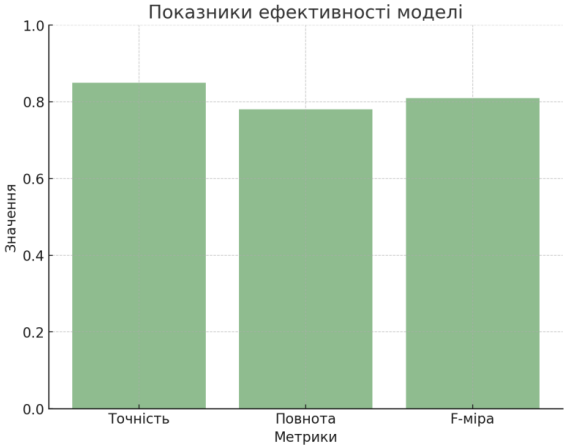

Рис. 1 – Показники ефективності моделі.

Розроблений алгоритм легко масштабовується та може бути використаний як окремий компонент у браузерному розширенні, у системі внутрішнього моніторингу трафіку компаній або як частина інтерактивного навчального інструменту з кібергігієни. Крім цього, він має потенціал до розвитку — у подальших роботах планується інтеграція моделей глибокого навчання для контентного аналізу, включення аналізу зображень та впровадження динамічного аналізу поведінки сторінки при взаємодії з користувачем.

Таким чином, створений інструмент є гнучким, адаптивним рішенням для реального виявлення шахрайських сайтів і дозволяє значно підвищити інформаційну безпеку користувачів у сфері електронної комерції.

1. Sabillon R., Cano M. J., Serra-Ruiz J., Cavaller V. Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security. 2016. Vol. 4. P. 165–176.
2. Zhang Y., Hong J. I., Cranor L. F. CANTINA: A Content-Based Approach to Detecting Phishing Web Sites. Proceedings of the 16th International Conference on World Wide Web (WWW'07). 2007. P. 639–648.
3. Marchal S., Saari K., Singh N., Asokan N. Know Your Phish: Novel Techniques for Detecting Phishing Sites and Their Targets. IEEE Transactions on Dependable and Secure Computing. 2017. Vol. 15(4). P. 594–607.

Модифікація квантового протоколу BB84 за допомогою системи залишкових класів

УДК 004.056.55

Анастасія Гнатюк[1], Михайло Касянчук[2], Павло Басістий[3]

[1,2]Західноукраїнський національний університет, [3]Тернопільський національний педагогічний університет імені Володимира Гнатюка,
[1]anastasia.hn88@gmail.com, [2]kasyanchuk@ukr.net, [3]basi@ukr.net

Квантова криптографія використовує принципи квантової механіки для встановлення каналів зв'язку між двома об'єктами і визначає методи безпечного спілкування через введення принципів квантової механіки для генерації ключів шифрування [1]. На відміну від класичної, квантова криптографія забезпечує свою безпеку через незмінні закони фізики, що призводить до її виняткової захищеності навіть відносно найскладніших обчислювальних систем [2].

Квантовий протокол розподілу ключів BB84 покладається на такі принципи квантової фізики:

1) принцип невизначеності Гейзенберга, який стверджує, що в квантовій системі можна точно визначити лише одну з пари спряжених величин, наприклад, координата та імпульс (вимірювання положення частинки призведе до порушення її швидкості). Квантова криптографія використовує це, застосовуючи поляризацію фотонів;

2) теорема про заборону клонування як наслідок попереднього принципу стверджує, що неможливо створити ідентичні копії невідомого квантового